مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

# Malicious Microsoft Teams Installers Delivering Oyster Backdoor

Tracking #:432317771

Date:03-10-2025



TLP: WHITE

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed researchers has identified an active campaign in which threat actors are distributing trojanized Microsoft Teams installers through SEO poisoning and malvertising techniques.

## TECHNICAL DETAILS:

Security researchers has identified an active campaign in which threat actors are distributing trojanized Microsoft Teams installers through SEO poisoning and malvertising techniques. Unsuspecting users searching for Microsoft Teams online are being redirected to spoofed domains serving a backdoored executable (MSTeamsSetup.exe). Once executed, the installer deploys the Oyster (a.k.a. Broomstick) backdoor, providing persistent remote access, system profiling, and delivery of additional payloads.

This campaign represents a continuation of earlier tactics used in fake PuTTY installer campaigns, demonstrating a persistent adversary trend of abusing trusted enterprise software brands to gain initial access and establish long-term persistence.

Oyster's stealthy DLL sideloading and scheduled task persistence mechanisms enable it to blend into normal enterprise workflows, making detection by traditional antivirus and some EDR solutions difficult.

**Key Findings**

- **Delivery Mechanism:** Attackers are using **SEO poisoning and malicious sponsored ads** to redirect users searching for Teams to spoofed domains (e.g., teams-install[.]top).
- **Malware Payload:** Users are served a **fake installer** (MSTeamsSetup.exe) signed with **untrustworthy digital certificates** to appear legitimate.
- **Persistence Technique:** Execution drops CaptureService.dll into %APPDATA%\Roaming, with a scheduled task ("CaptureService") invoking it regularly via rundll32.exe.
- **Backdoor Capabilities:** Oyster provides:
  - Persistent **remote access**
  - **System profiling & host reconnaissance**
  - **Follow-on payload delivery**
  - Stealth execution that blends with normal Windows processes
- **C2 Infrastructure:** Observed communicating with attacker-controlled domains nickbush24[.]com and techwisenetwork[.]com.
- **Trend Continuation:** Mirrors prior **fake PuTTY installer campaigns**, showing a recurring attacker pattern of exploiting trust in popular software.
- **Detection Gap:** Campaign has **bypassed certain AV/EDR solutions**, highlighting the need for layered defenses.

**Indicators of Compromise:**

| IOCs | Type | Description |
|---|---|---|
| 9dc86863e3188912c3816e8ba21eda939107b8823f1afc190c466a7d5ca708d1 | SHA256 | MSTeamsSetup.exe |

| | | |
|---|---|---|
| bc8cd78ade90511d488823e289eed30708d275f9 | SHA1 | MSTeamsSetup.exe |
| 94297d9999a734593e53da1fe28e38bc | MD5 | MSTeamsSetup.exe |
| ac5065a351313cc522ab6004b98578a2704d2f636fc2ca78764ab239f4f594a3 | SHA256 | MSTeamsSetup.exe |
| e7f8da0b97f4207738ce895ef15be4133122b307 | SHA1 | MSTeamsSetup.exe |
| d5ecd8120b6a107513b9871ec0475ace | MD5 | MSTeamsSetup.exe |
| d47f28bf33f5f6ee348f465aabbfff606a0feddb1fb4bd375b282ba1b818ce9a | SHA256 | CaptureService.dll |
| e0a2cb7450b0d71d03e07d76fefa9c0555b8e931 | SHA1 | CaptureService.dll |
| 5325f705e2195f49df0fdc41af6934b0 | MD5 | CaptureService.dll |
| d46bd618ffe30edea56561462b50eb23feb4b253316e16008d99abb4b3d48a02 | SHA256 | CaptureService.dll |
| 8d8ceba1b31f4ace5a9c44225014d3947fbf205a | SHA1 | CaptureService.dll |
| d28b4136a7e6148de5c26a055c711f4f | MD5 | CaptureService.dll |
| 90b633cacfa185dd912a945f370e14191644ecff1300dbce72e2477171753396 | SHA256 | Ads.dll |
| team[.]frywow[.]com | Domain | Malvertising Domain |
| teams-install[.]icu | Domain | Malvertising Domain |
| teams-install[.]top | Domain | Malvertising Domain |
| nickbush24[.]com | Domain | Oyster C2 |
| techwisenetwork[.]com | Domain | Oyster C2 |
| maddeehot[.]online | Domain | Oyster C2 |
| server-na-qc2[.]farsafe[.]net | Domain | Oyster C2 |
| 45.66.248[.]112 | IP | Oyster C2 |
| 54.39.83[.]187 | IP | Oyster C2 |
| 185.28.119[.]228 | IP | Oyster C2 |

## RECOMMENDATIONS:

- **Enforce Trusted Download Sources**
  - Ensure users download collaboration and administrative tools only from official vendor websites or trusted internal software repositories.
  - Block access to known malicious domains via DNS/web filtering.
- **User Awareness & Training**
  - Conduct awareness campaigns to warn staff about the dangers of downloading software via search engine results or sponsored ads.

- Reinforce the use of bookmarked links for critical tools like Microsoft Teams.

- **Endpoint Detection & Response (EDR)**
  - Deploy and maintain EDR solutions capable of detecting modular malware, suspicious installer behavior, and DLL sideloading techniques.
  - Tune detection rules to flag execution chains involving rundll32.exe launched by installers.
- **Network Monitoring**
  - Implement network monitoring to detect encrypted outbound traffic to unrecognized or suspicious domains.
  - Regularly review proxy/DNS logs for connections to attacker-controlled infrastructure (e.g., nickbush24[.]com, techwisenetwork[.]com).
- **Persistence & Process Monitoring**
  - Monitor for new scheduled tasks created under %APPDATA%, especially tasks named CaptureService.
  - Alert on rundll32.exe loading DLLs from non-standard directories such as %APPDATA%\Roaming.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERNCES:


- https://blackpointcyber.com/blog/malicious-teams-installers-drop-oyster-malware/